This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

REMARKS

This is in response to the Office Action mailed on April 30, 2004. The Office Action rejected Applicant's Claims 1-16, 18-32 and 34-39 as being anticipated by U.S. Pat. No. 6,314,409 ("Schneck"). The Office Action rejected Claims 17 and 33 as obvious in view of the combination of Schneck and U.S. Pat. No. 5,887,269 ("Brunts"). The Office Action objected to Claim 15 for informalities.

With this response, Claims 1, 8, 9 and 15 have been amended. Applicant respectfully requests the Examiner to reconsider the present application. Applicant submits that all pending claims are in condition for allowance.

Claim 15

Applicant has amended Claim 15 as suggested by the Examiner correcting "date" to "data."

Independent Claim 1

Applicant's independent Claim 1 relates to a method of securely conveying a data product. Amended Claim 1 recites "verification information" that "includes a data storage medium ID" and the "data storage medium ID is used to validate that a data storage medium is authorized to store the data product." Claim 1 is not anticipated by Schneck because Schneck fails to disclose all of the recited claim elements.

Briefly, Schneck discloses a system for a controlling access to data. The Schneck system includes an authorizing mechanism to produce packaged data that includes access rules. (*see*, Schneck: column 9, lines 61-65). The access rules enable the user to access the data of the packaged data in various controlled ways. (*see*, Schneck: column 10, lines 3-5). The rules include validity checking and identification information such as version number, license number. (*see*, Schneck: Fig. 3, column 11, lines 4-48). The rules also include access control parameters that define allowed and disallowed actions with the data, such as no modify, no child access, and access cost. (*see*, Schneck: column 23, lines 10-65).

Although Schneck discloses some access rules, Schneck fails to disclose or suggest a data storage medium ID as verification information and that the data storage medium ID is used to validate that a data storage medium is authorized to store the data product. Although Schneck stores the encrypted access rules on a storage medium, the access rules do not include a data storage medium ID that is used to validate whether a storage medium is authorized to store the data package. Rather, Schneck merely discloses access rules that determine whether and how a user (system) may access the data from any storage medium, not whether the storage medium is authorized to store the data product. In fact, Schneck teaches away from this claim element because Schneck assumes that all storage medium can store the packaged data and Schneck controls access to the data using the access rules regardless of the storage medium.

For at least the above reasons, Claim 1 is not anticipated by Schneck. Thus, independent Claim 1 is in condition for allowance.

<u>Independent Claim 11</u>

Applicant's independent Claim 11 relates to a method of securely conveying data. Claim 11 recites "computing a first checksum of the set of authorization parameters," "using the first cryptographic key" to "encrypt the set of authorization parameters" and "encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value." Claim 11 is not anticipated by Schneck because Schneck fails to disclose all of the recited claim elements.

Briefly, Schneck discloses a system for a controlling access to data. The Schneck system includes an authorizing mechanism to produce packaged data that includes an encrypted body part, unencrypted body part, encrypted rules and encrypted ancillary information. (*see*, Schneck: Fig. 2, column 11, lines 61-65, column 10, lines 47-54). The authoring mechanism selects a data-encryption algorithm and data-encrypting key and then the authoring mechanism encrypts the data-encrypting key with a rule-encrypting key. The encrypted data-encrypting key is then stored in the encrypted ancillary information of the packaged data. (*see*, Schneck: column 12, lines 32-38). Next, the other elements of the

PAGE 13/17 * RCVD AT 7/30/2004 4:40:24 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:13128947228 * DURATION (mm-ss):05-58

data are processed and encrypted using the data-encrypting key including the ancillary information and body part of the data and stored in their respective part of the data package. The rules are encrypted with rule-encryption key and stored in the encrypted rules part of the data package. (*see*, Schneck: column 13, lines 11-16, 25-29, 34-39).

Although Schneck discloses access rules and ancillary information for the packaged data, Schneck fails to disclose or suggest computing a first checksum of the set of authorization parameters. Schneck merely discloses developing access rules that determine whether and how a user may access the data and ancillary data that identifying the packaged data. Additionally, Schneck fails to disclose or suggest encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value. Although Schneck discloses encrypting the access rules similar to claim element of "encrypt the set of authorization parameters," Schneck fails to disclose or suggest the further claim element of encrypting a combination of the first cryptographic key and the first checksum so as to produce a header value. In fact, Schneck teaches away from the claim element by encrypting the decryption key and access rules separately.

For at least the above reasons, Claim 11 is not anticipated by Schneck. Thus, independent Claim 11 is in condition for allowance.

Independent Claim 14

Applicant's independent Claim 14 relates to a method of securely conveying data. Claim 14 recites "verification information indicative of a data storage medium on which the data is authorized to be stored" and "to determine, by reference to the verification information whether the given storage medium is the data storage medium on which the data is authorized to be stored." Claim 14 is not anticipated by Schneck because Schneck fails to disclose all of the recited claim elements.

Briefly, similarly as discussed above in conjunction with Claim 1, Schneck fails to disclose or suggest verification information indicative of a data storage medium on which the data is authorized to be stored and to determine whether the given storage medium is the data storage medium on which the data is authorized to be stored. Although Schneck stores the encrypted access rule on a storage medium, the access rules do not include information whether the given storage medium is authorized to store the data package. Rather, Schneck merely discloses access rules that determine whether and how a user (system) may access the data from any storage medium, not whether the storage medium is authorized to store the data product. In fact, Schneck teaches away from this claim element because Schneck assumes that all storage medium can store the packaged data and Schneck controls access to the data using the access rules regardless of the storage medium.

For at least the above reasons, Claim 14 is not anticipated by Schneck. Thus, independent Claim 14 is in condition for allowance.

Independent Claim 16

Applicant's independent Claim 16 relates to a method of securely communicating a data product. Claim 16 recites "computing a first value as a first function of input parameters including (i) an identification code and (ii) a second value," "combining the first value with the first cryptographic key to produce a third value," "adding the third value to the authorization key," "using the first value as a second cryptographic key" and "encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key." Claim 16 is not anticipated by Schneck because Schneck fails to disclose all of the recited claim elements.

Briefly, Schneck discloses a system for a controlling access to data. The Schneck system includes an authorizing mechanism to produce packaged data that includes an encrypted body part, unencrypted body part, encrypted rules and encrypted ancillary information. (*see*, Schneck: Fig. 2, column 11, lines 61-65, column 10, lines 47-54). The authoring mechanism selects the rule-encrypting key as a function of the validated serial number. (*see*, Schneck: column 14, lines 45-53). The authoring mechanism selects a data-encryption algorithm and data-encrypting key and then the authoring mechanism encrypts the data-encrypting key with a rule-encrypting key. The encrypted data-encrypting key is then stored in the encrypted ancillary information of the packaged data (*see*, Schneck:

column 12, lines 32-38). Next, other elements of the data are processed and encrypted using the data-encrypting key including the ancillary information and body part of the data and stored in their respective part of the data package. The rules are encrypted with rule-encryption key and stored in the encrypted rules part of the data package. (*see*, Schneck: column 13, lines 11-16, 25-29, 34-39).

Although Schneck discloses computing the rule-encrypting key, Schneck fails to disclose or suggest computing the first value that is used as a second cryptographic key as a function of the identification code and a second value. Rather, Schneck merely discloses computing the rule-encrypting key computing as a function of a serial number, not identification code and a second value. Furthermore, Schneck fails to disclose the second value and encrypting the second value to produce an encrypted value that can be decrypted using a third cryptographic key. Schneck merely discloses two keys – data encrypting key and rule-encrypting key – not a third key. Additionally, Schneck fails to disclose or suggest "combining the first value with the first cryptographic key to produce a third value" and "adding the third value to the authorization key."

For at least the above reasons, Claim 16 is not anticipated by Schneck. Thus, independent Claim 16 is in condition for allowance.

Independent Claim 27

Applicant's independent Claim 27 relates to a method of securely a data product. Claim 27 recites "computing a first value as a first function of input parameters including (i) an identification code and (ii) a second value," "combining the first value with the first cryptographic key to produce a third value," "adding the third value to the authorization key," "using the first value as a second cryptographic key" and "encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key." For the reasons discussed in conjunction with Claim 16, Claim 27 is not anticipated by Schneck. Thus, independent Claim 27 is in condition for allowance.

Claims 2-10, 12-13, 15, 17-26 and 28-39

Applicant's Claims 2-10, 12-13, 15, 17-26 and 28-39 are dependent claims that distinguish the cited references for at least the same reasons explained above in conjunction with their independent base claims. In addition, these claims recite further features and claim elements that are neither disclosed nor suggested by the cited references.

Conclusions

Applicant submits that all the pending claims in the present application are allowable and that the present application is in condition for allowance. If any issues remain in the present application, the Examiner is requested to call the undersigned at the telephone number below.

Respectfully submitted,

Jon D. Shutter
Reg. No. 41,311
Patent Counsel

NAVTEQ North America, LLC
222 Merchandise Mart Plaza Drive, Suite 900
Chicago, IL 60654
(312) 894-7000 x7365